PELCO®

Important Security Information for System Administrators

DX8100 Digital Video Recorder

C2641M-A (9/07)

Contents

List of Illustrations

List of Tables

DX8100 Platform Security Information

The DX8100 Series digital video recorder (DVR) is equipped with an extensive set of security measures to provide the user with secure, uninterrupted service.

NOTE: While great care has been taken in the design and development of the DX8100 to ensure a secure DVR platform, it is not feasible to protect a system from all internal and external security risks if it is connected to an unsecured network. In addition to the robust security features built into the DX8100, you should consult with your network administrator, information technology department, and facilities manager to ensure that all possible measures are being taken to ensure the safety and security of the DX8100 and its data.

The following sections describe the security features of the DX8100 in detail. These sections are intended for system administrators who are responsible for the maintenance and security of the DX8100.

PHYSICAL SECURITY

Like any other video recording device, including VCRs, the security of the DX8100 is largely dependent on the physical security of the unit itself. When an intruder has access to the hardware, it will be possible to remove components and retrieve recorded data. Units should therefore be installed in a location that is physically secured.

Because the dimensions and underlying technologies of the DX8100 are similar to those of a modern personal computer, it is possible to rack mount units and access the mouse and keyboard inputs using commercially available keyboard video mouse (KVM) switches. This may bring the control of the units outside of the secured area. One area where this could cause a problem involves access to the system's basic input/output system (BIOS). Pelco recommends that the unit be given a BIOS supervisor password upon completion of installation. A unique BIOS supervisor password will help prevent remote operators from changing boot parameters that could allow the unit to be booted using unsecured sources.

The DX8100 is engineered to reboot automatically in the event of a system problem. The capability of recovering from certain errors without operator intervention minimizes the potential amount of time a DVR will be offline. To retain this capability, it is important that a password be set for BIOS Supervisor account only and not for the BIOS User account. Setting a password for the BIOS User account would force operators to re-enter this password each time the system is rebooted.

⚠ **WARNING:** Always scan removable media, such as CD-RW and DVD-RW disks, for viruses before inserting them into the DX8100.

SETTING THE BIOS SUPERVISOR PASSWORD

The following procedure describes how to set the BIOS supervisor password. This procedure should be performed only by advanced users with extensive experience with PC computer technology. Changing BIOS settings to incorrect values may result in the degradation of system performance or cause your DVR to stop working.

To set the BIOS supervisor password:

1. Boot the DX8100 Series DVR by turning on the power switch.

2. Press the Delete key on the keyboard as soon as the Pelco splash screen is displayed. The BIOS Main screen opens.

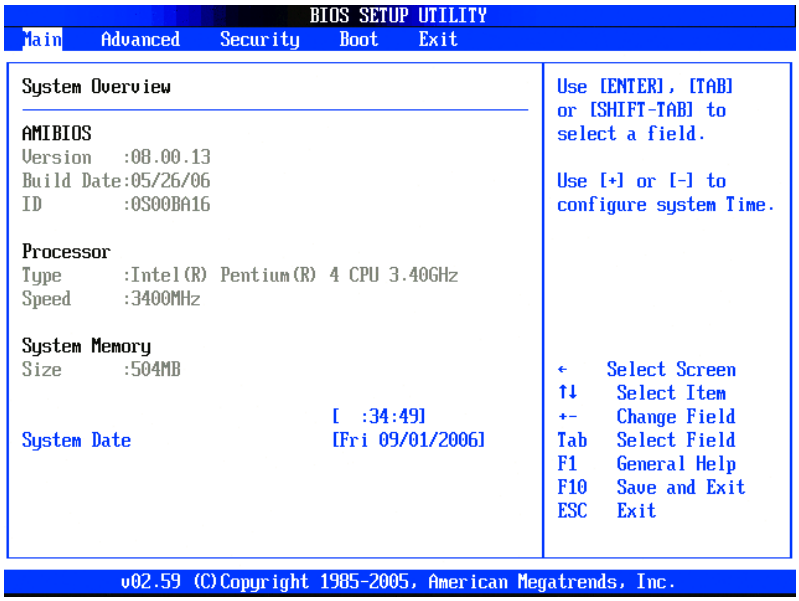

Figure 1. DX8100 BIOS Setup Main Screen

3. Use the cursor control keys on your keyboard to move over to the Security tab and select Change Supervisor Password.
4. Press the Enter key on your keyboard. The Enter New Password dialog box opens.
5. Enter a new password for the BIOS Supervisor account. Passwords should be between four to six alphanumeric characters.
6. Press Enter to accept the new password.

⚠ **WARNING:** Make sure that you only set the BIOS supervisor password. Do not assign a password to the BIOS user password.

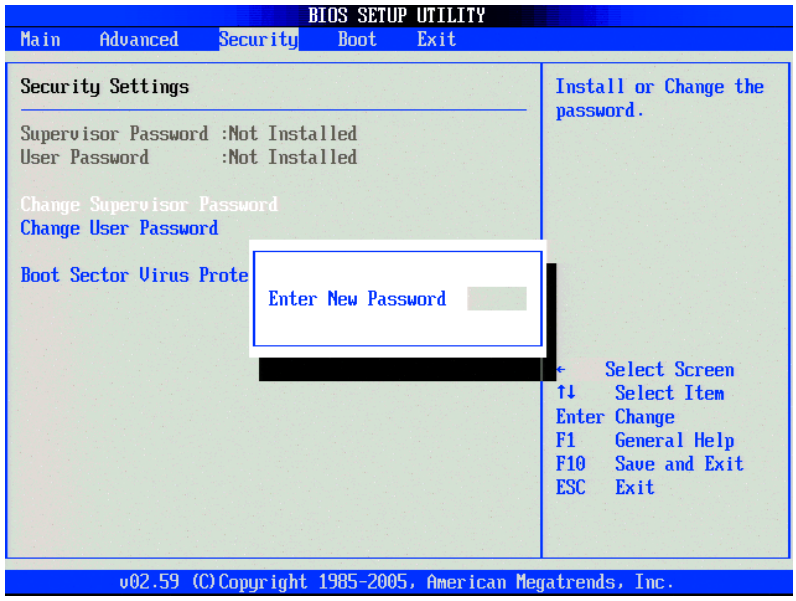

Figure 2. New BIOS Password Dialog Box

7. Re-enter the password to confirm that it is correct.
8. Press Enter to confirm the new password.

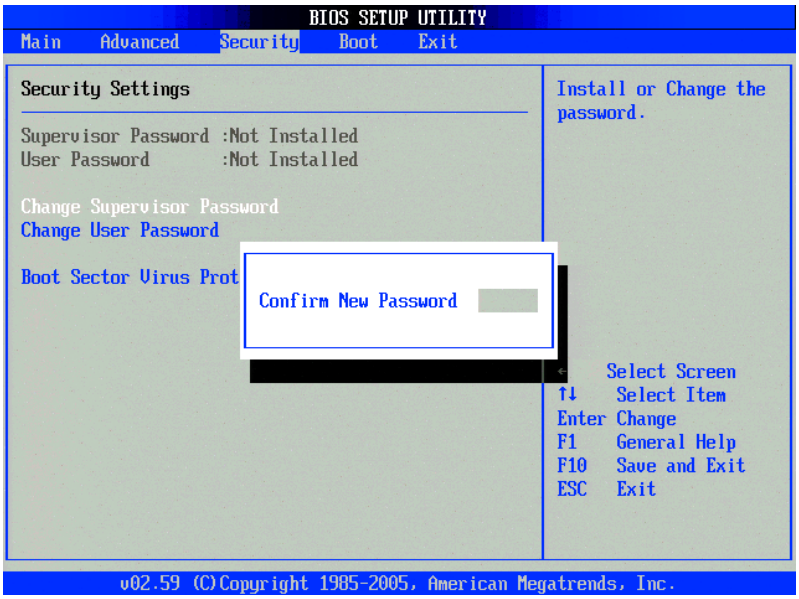

Figure 3. Password Confirm Dialog Box

NOTE: Remember to write down this password and keep it in a secure place.

9. Press the F10 function key on your keyboard to save and exit the BIOS setup screen.
10. Finalize BIOS changes:
    - To accept the BIOS changes and reboot, press the Enter key.
    - To cancel the BIOS changes, press the Esc key and Ctrl+Alt+Delete to reboot the DX8100.

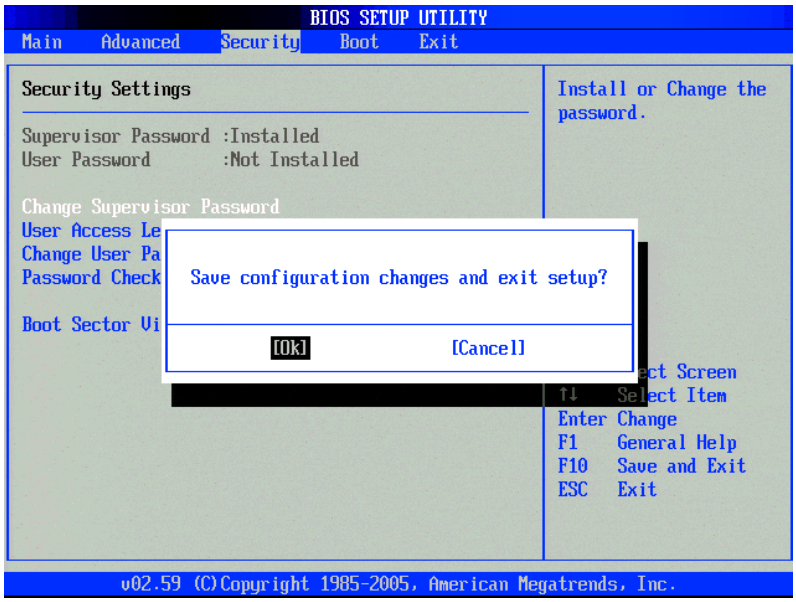

Figure 4. BIOS Setup Confirmation Screen

OPERATING SYSTEM SECURITY

Upon a successful boot procedure, the DX8100 will automatically load the Windows® 2000 or Windows XP Embedded operating system. These operating systems are specifically tailored for use on the DX8100. It does not have the standard feature set found in the commercially available version of the Windows 2000 or Windows XP Embedded operating system. This means that services that are not needed for the correct operation of the DX8100 have been removed to eliminate potential vulnerabilities.

Only two user accounts are available in the DX8100's operating system software. These user accounts should not be confused with the accounts assigned by the DX8100 application software. An administrator account allows a designated user to make changes to the registry and security settings to accommodate the requirements of the specific site.

In finding a balance between security and functionality, Pelco has consistently opted for security but leaves it up to the administrator to unlock features that might be useful if the administrator has determined that the additional security of the lockdown is not needed. A typical example of this is the capability of the DX8100 to use dynamic IP addresses. Because IP addresses can change over time, clients must use a different mechanism to connect to the server than by simply providing an IP address. The additional use of NetBIOS protocol services allows the computer to find IP addresses on the local LAN by system name; it should be noted that this also creates a known vulnerability. To allow the end user to use the NetBIOS feature, the services are activated at the factory, but they can be disabled by an administrator when needed. When NetBIOS services are activated, the administrator needs to apply alternative means to protect against hackers and viruses such as a firewall. Please check with your information technology specialist or contact Pelco Product Support for further instructions.

WINDOWS OPERATING SYSTEM UPDATES

Due to the lockdown of nonessential services on the DX8100, administrators are advised against installing every operating system upgrade published by Microsoft®. The majority of these updates are not applicable to the DX8100. Pelco will provide a list of approved updates upon request.

WINDOWS 2000: CHANGING THE ADMINISTRATOR PASSWORD

This section describes how to change the Windows administrator password. The DX8100ADM password should be changed immediately upon installation of the DX8100 DVR. If the DX8100ADM account is not properly password protected, your system will be highly vulnerable to damage and improper use from a variety of security threats.

Before attempting to access or change the DX8100ADM account, be aware that only authorized personnel with advanced technical experience working with the Windows 2000 operating system should log on to or change the DX8100ADM account. Damage to the DX8100, its system and application software, and loss of critical data may result from improper use of the DX8100ADM account. You must have the Windows password to exit from the DX8100 application to the Windows operating system. The Windows default password is dx8100.

To change the Windows 2000 DX8100ADM password:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Windows Control Panel opens.

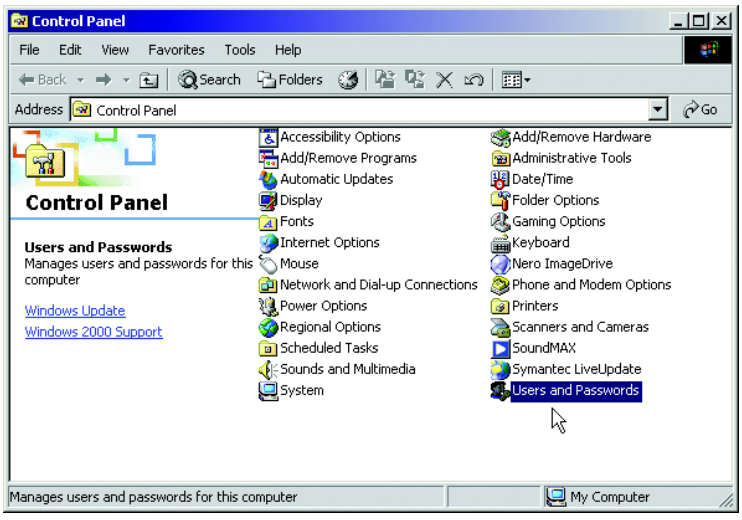

Figure 5. Users and Passwords Icon in Control Panel

3. Double-click the Users and Passwords icon. The User and Passwords dialog box opens.

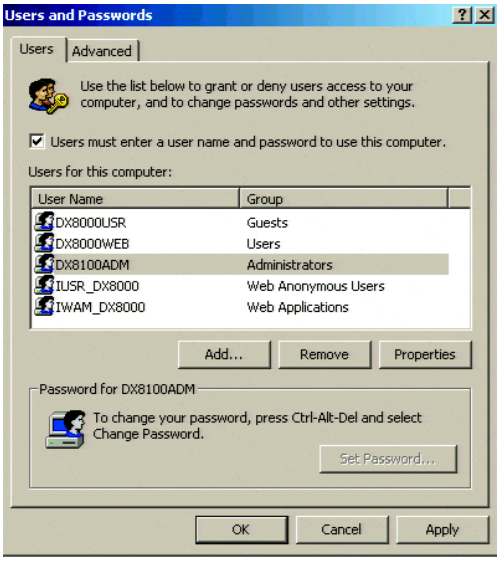

Figure 6. Users and Passwords Dialog Box

4. Click the Advanced tab. The Advanced page opens.

Figure 7. Advanced Page

5. Click the Advanced button. The Local Users and Groups dialog box opens.

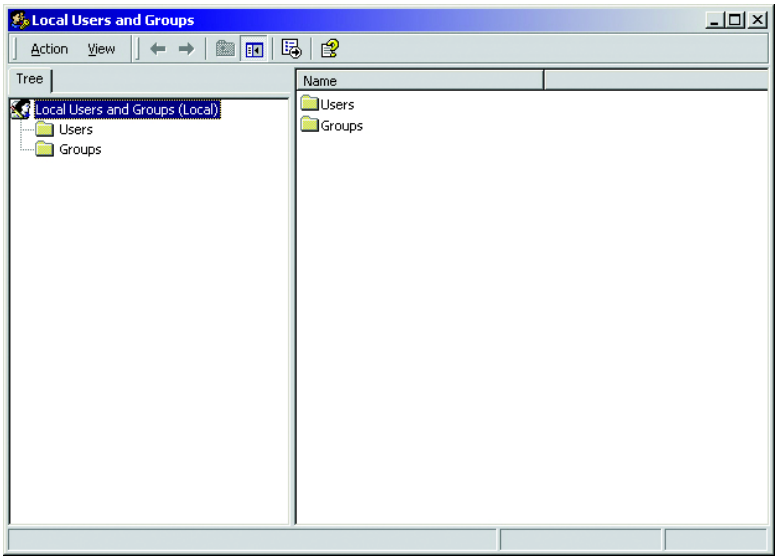

Figure 8. Users and Groups Dialog Box

6. Click Users.

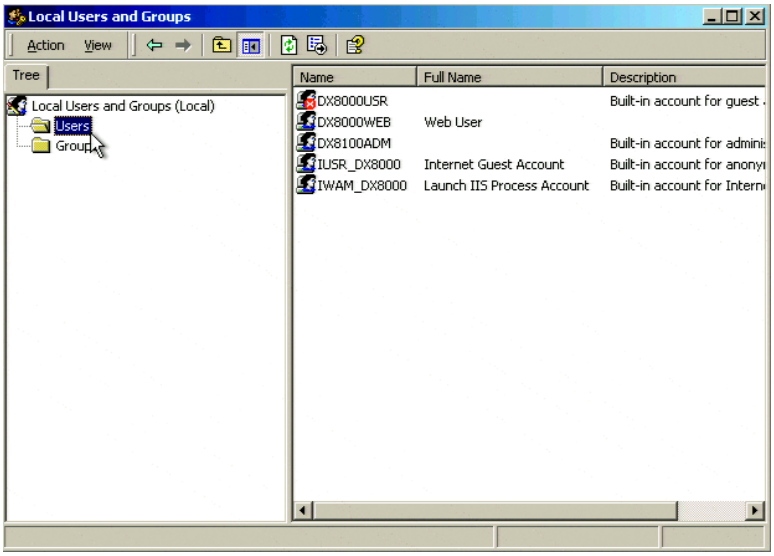

Figure 9. User Listing Dialog Box

7. Right-click DX8100ADM and then select the Set Password option from the shortcut menu.

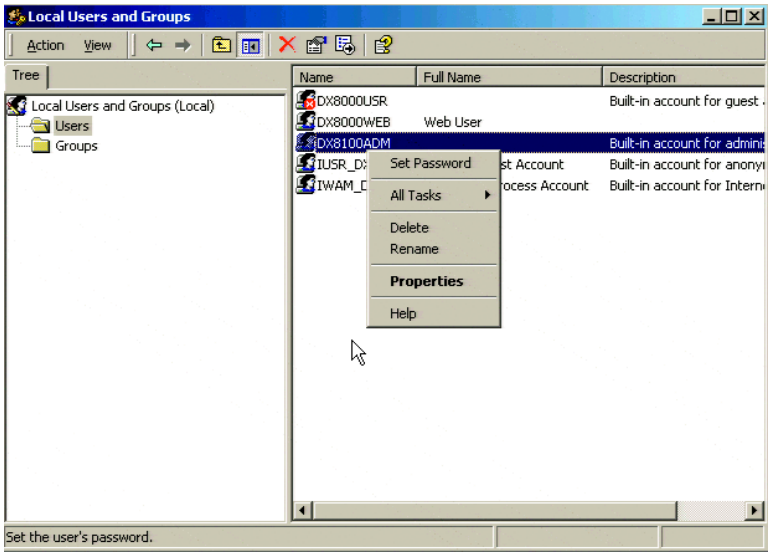

Figure 10. Enter and Confirm New Password

The Set Password dialog box opens.

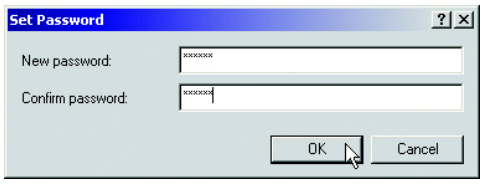

Figure 11. Set Password Dialog Box

8. Enter a new password for the DX8100ADM account. Passwords are case-sensitive and should contain a mixture of alphabetic and numeric characters between six and ten characters in length.

   NOTE: Remember or write down this password and keep it in a secure place.

9. Click OK. The Set Password dialog box closes.
10. Close the Local Users and Groups dialog box and click OK.
11. Click Start > Shutdown > Restart to reboot the DX8100. The Log On to Windows Dialog Box opens.

Figure 12. Log On to Windows Dialog Box

12. Enter the new password and click OK. The DX8100 server application opens.

To enable the automatic logon feature:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Control Panel dialog box opens.
3. Double-click Users and Passwords icon. The Users and Passwords dialog box opens.

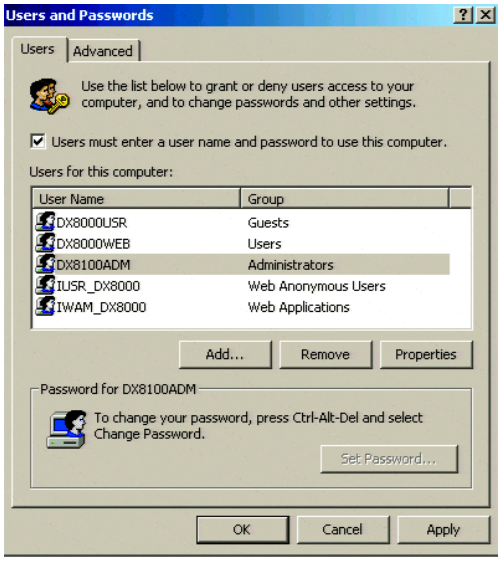

Figure 13. Users and Passwords Dialog Box

4. Click the check box "Users must enter a user name and password to use this computer."
5. Click the check box again to deselect it and then click Apply. The Automatically Log On dialog box opens.

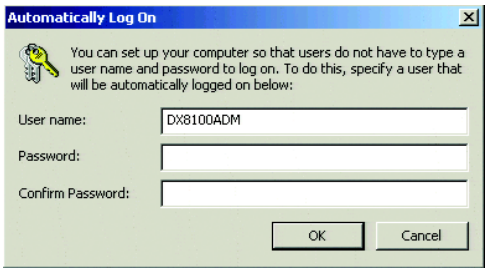

Figure 14. Automatically Log On Dialog Box

6. In the Password text box, type the new DX8100ADM password.
7. In the Confirm Password text box, retype the password again.
8. Click OK and then restart the DX8100 server. The unit will restart and automatically log you on to the DX8100 server application.

WINDOWS XP EMBEDDED: CHANGING THE ADMINISTRATOR PASSWORD

To change the Windows XP Embedded DX8100ADM password:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Click Start > Settings > Control Panel. The Windows Control Panel opens.

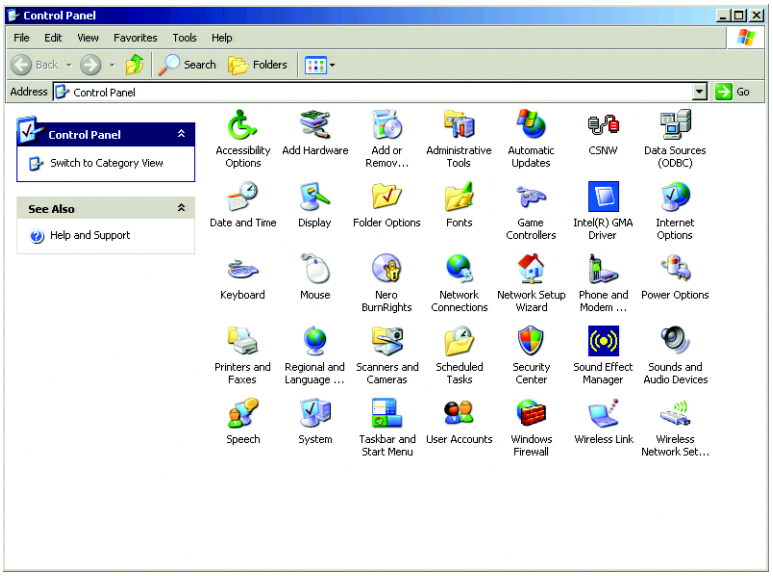

Figure 15. Users and Passwords Icon in Control Pane

3. Double-click the User Accounts icon. The User Accounts dialog box opens.

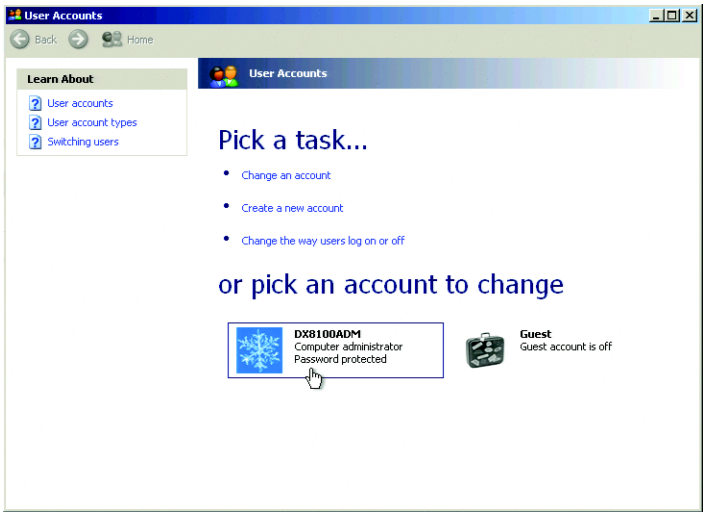

Figure 16. User Accounts Dialog Box

4. In the accounts list, click the DX8100ADM account. The User Accounts dialog box displays “What do you want to change about your account?”

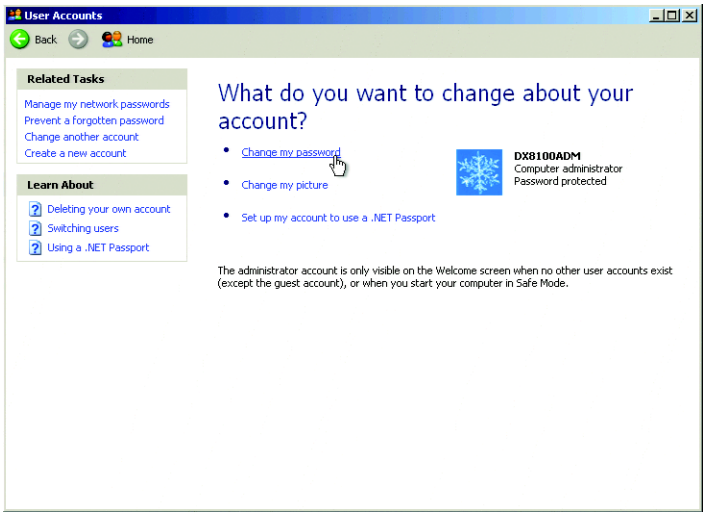

Figure 17. Changing Your Account Prompt

5. Click “Change my password.” The “Change your password” dialog box opens.

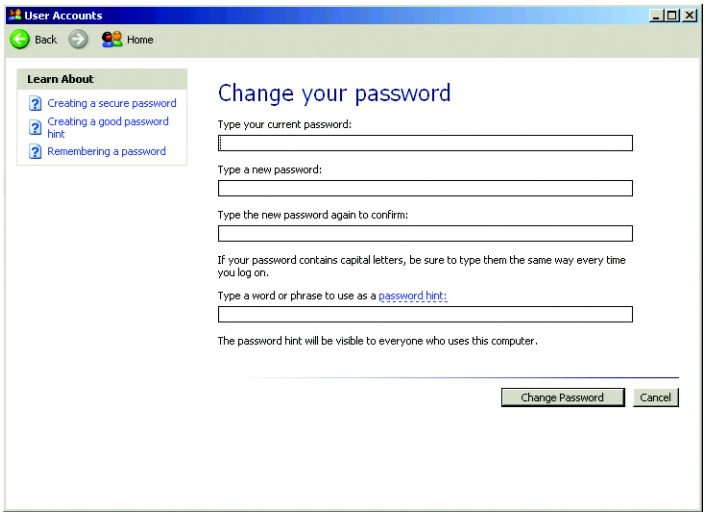

Figure 18. Change Your Passwords Dialog Box

6. Enter the new password for the DX8100ADM account and then click the Change Password button. A prompt is not displayed advising you that the password is been changed. Instead, the dialog box closes and the User Accounts “Pick a task” dialog box is redisplayed.

   Passwords are case-sensitive and should contain a mixture of alphabetic and numeric characters between six and ten characters in length.

   NOTE: Remember or write down this password and keep it in a secure place.

7. To log on to the DX8100 server application, do one of the following:
   - To manually log on, go to step 8.
   - To enable automatic log on, refer to *Enabling Automatic Logon* on page 16.

8. To manually log on to the server application:

   a. Close the User Accounts dialog box, and then restart the DX8100. The logon message dialog box opens.

   b. Click OK. The Log On to Windows dialog box opens.

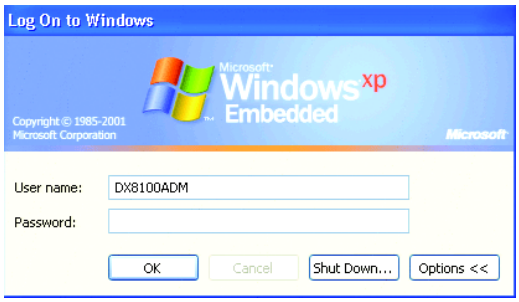

Figure 19. Log On to Windows Dialog Box

   c. Enter the new password and then click OK. The DX8100 server application starts.

ENABLING AUTOMATIC LOGON

The DX8100 can be configured to automatically log on to the server. If the password is changed, this feature is disabled. To reactivate the automatic logon feature, you must reconfigure the unit each time the password is changed.

1. To reconfigure the automatic logon, do one of the following:
   - In the Windows environment, go to step 2.
   - In the DX8100 application, exit the DX8100 application, and return to the Windows operating system.
2. To configure the DX8100 to automatically log on to the server application:

   a. On the taskbar, click Start and then click Run. The Run dialog box opens.

   b. In the Open text box, type **control userpasswords2**.

   c. Click OK. The User Accounts dialog box opens.

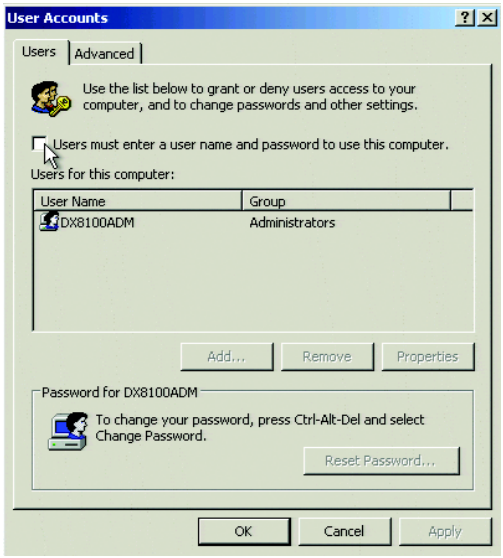

Figure 20. User Accounts Dialog Box

   d. Click the check box "Users must enter a user name and password to use this computer."

   e. Click the check box again to deselect it and then click Apply. The Automatically Log On dialog box opens.

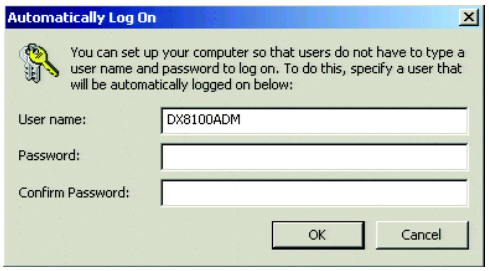

Figure 21. Automatically Log On Dialog Box

f. In the Password text box, type the new DX8100ADM password.

g. In the Confirm Password text box, retype the password again.

h. Click OK and then restart the DX8100 server. The unit will restart and automatically log you on to the DX8100 server application.

ENABLING CTRL+ALT+DEL

Enabling the Ctrl+Alt+Del key combination allows you to open the Windows Task Manager dialog box to perform Windows system administration tasks. To complete the procedure, you must be logged on to the DX8100 application as the Admin user. The standard Ctrl and Alt keys are remapped for the DX8100 application, refer to Table A. The key combination used to implement Ctrl+Alt+Del is F2+F9+Del.

Table A. Keyboard Remapping

DX8100 Key	Windows Action
F2	Ctrl
F4	Space
F9	Alt
Ctrl	Space
Alt	Space

To enable the Ctrl+Alt+Del key feature:

1. Click the Setup button  .
2. Click the System button  .
3. From the Setup Ctrl + Alt + Del key combination area, click the Enable Ctrl+Alt+Del key combination selection check box.
4. Click Apply.
5. Reboot the DX8100.

USING F2+F9+DEL

The Ctrl+Alt+Del feature must first be enabled. F2+F9+Del allows you to access the Windows Task Manager dialog box from within the DX8100 shell. When you exit the Windows environment, you are returned to the DX8100 shell. In this case, you do not have to log on to the unit again.

To access the Windows Task Manager dialog box:

1. Press F2+F9+Del. The Windows Security dialog box opens.
2. In the Windows Security dialog box, click Task Manager. The Windows Task Manager window opens.
3. To return to the DX8100 shell without rebooting the DX8100, exit the Windows Task Manager dialog box.

DX8100 SECURITY

INTERNET PROTOCOL SECURITY

The DX8100 features built-in network security using Internet Protocol Security (IPSec). IPSec facilitates authentication and encryption at the network packet level. IPSec services protect the DX8100 from unwanted or potentially damaging network requests. With IPSec enabled, the DX8100 DVR will not respond to any unsecured communication across the network, whether friendly or malicious. IPSec only blocks unwanted or unauthorized communication flowing to the DX8100. It does not hinder communication sessions that are initiated by the DVR.

IPSec is enabled by default on the DX8100; however a system administrator can disable the service if it is deemed necessary for the proper functioning of the unit.

⚠ **WARNING:** Disabling IPSec services will expose your DX8100 Series DVR to potentially damaging network traffic. It is highly recommended that IPSec is enabled at all times for the protection of your system.

To disable IPSec services on the DX8100 Series DVR:

1. Exit the DX8100 application if it is running, and return to the Windows operating system.
2. Go to Start > Programs > Manage IPSec Policy. The DX8100 IPSec Policy dialog box opens.

Figure 22. DX8100 IPSec Policy Dialog Box

3. Deselect the Enable DX8100 IPSec Policy check box. Reselect the Enable DX8100 IPSec Policy check box to re-enable IPSec.
4. Click OK.

FIREWALLS

The DX8100 includes the Windows firewall that comes with Service Pack 2 for Windows XP. The security services provided by the Windows Firewall protects the DX8100 from unwanted or potentially damaging network requests. With the Windows Firewall and IPSec enabled, the DX8100 DVR will not respond to any unsecured communication across the network. However, there are potential risks to which you should be aware. The Windows Firewall does not block all ports. For a list of ports required for operation, refer to *DX8100 Network Ports* on page 19.

Pelco recommends that an external network firewall be used. The network firewall will provide additional protection for the DX8100. Regardless of which port or service is under attack, the port must be open or at least visible in order for the malicious program to exploit it. Firewalls filter and render all unneeded ports invisible, providing excellent protection against such attacks. Networked systems exposed in anyway to the outside world (for example, when connected to the Internet) should be equipped with network-based firewall protection.

DX8100 NETWORK PORTS

Table B describes the DX8100 ports and their functions. The ports are classified either as user-changeable or fixed. You can assign a user-changeable port a different number. In this case, a port's number must be assigned within the range of 5000–65535. If a port is assigned out of this range, the system displays a message alerting you that an invalid port number is being used. You cannot assign a different number to a fixed port.

Table B. Open Ports on the DX8100

PORT	User-Changeable	Function
80/tcp	No	HTTP (Hyper Text Transfer Protocol) forms the basis for Web page transfer over the Internet. Ports 1–255 are reserved for well-known services at network communication
135/tcp, udp	No	End Point Mapper (EPMAP), a Microsoft RPC locator service
137/tcp, udp	No	File/print sharing (NetBIOS name service)
1028/tcp	No	Remote Procedure Call (RPC)
1801/tcp	No	Message queuing
1900/udp	No	Universal plug-and-play (UPnP)
2103/tcp	No	Message queuing
2105/tcp	No	Message queuing/logon
2107/tcp	No	Message queuing
2869/tcp	No	UPnP
9002/tcp	Yes	DX8100 base port, used for transmission of video, audio, and interface data
9003/tcp	Yes	DX8100 software upgrade port, used for remote upgrade of DX8100 software
9005/tcp	Yes	DX8100 information port

NOTE: Unless there is a conflict on your network, it is recommended that you do not change port numbers from their default settings. Make sure any changes to port numbers are made consistently across all DX8100 servers and clients on a network.Client and server ports must be identical.

The DX8100 port functionality is summarized as follows:

- **Base port:** This port is configured at the DX8100 Network setup screen. The base port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site setup screen.
- **Software Upgrade Port:** This port is configured at the DX8100 Network setup screen. The upgrade port number is downloaded to the PC client system during an IP scan. The port number can be modified at the DX8100 Site setup screen. The PC client's upgrade port number must match the DX8100 server's upgrade port number. For server-to-server software upgrades, both server software upgrade port numbers must match.
- **Agent Port:** This port is configured at the DX8100 Notification setup screen. You change the client emergency agent server listening port using the Emergency Agent application running on the PC client system. For more information about changing the client emergency agent listen port, see the Client Applications manual.
- **Other reserved ports:** Ports 256–1023 are reserved for well-known services. Ports 1024–4999 are temporal client ports (OS allocates automatically).

APPLICATION SOFTWARE

The only application intended and guaranteed to work on the unit is the DX8100 application software itself. Do not install other application software. If you do, this voids the warranty on the unit, and it also opens up potential holes in the system security. The DX8100 application software has several user and group accounts with varying degrees of rights and permissions on the system. Each account is password-protected. These accounts and passwords are completely different from the operating level account and password discussed in the previous section. The typical system operator will have to work only with application program level user names and passwords.

PASSWORD RECOVERY

There are no “backdoor” accounts or alternative access options built into the DX8100 application software. Pelco cannot issue overriding passwords, factory passwords, or other means to bypass the logon requirement of the application program. If the DX8100´s Admin account password is lost or forgotten, there is only one method for resetting the Admin password without completely reinstalling the system from the Recovery CD.

Upon request, Pelco can issue a unique password recovery code that is valid for 24 hours only. The recovery code is exclusive to the machine for which it is issued. If needed, the original buyer of the system (typically the dealer) may contact Pelco Product Support with the serial number and order or invoice number on which the unit was originally purchased. This must be done in writing, and the request must be accompanied by a letter from the current owner of the system stating the he or she is the legal owner of the system, the password for the system was lost, the MAC address for the DVR(s) for which a reset code is needed, and that he or she is requesting a password reset code. Upon verification, Pelco will issue a reset code that can be used for 24 hours on the DX8100 with the provided MAC address only.

To recover a lost or forgotten Admin password:

1. Go to File > Password Recovery. The Password recovery dialog box opens.

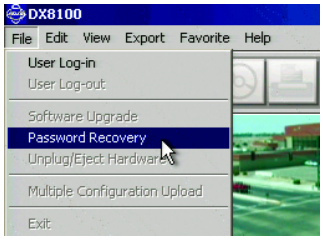

Figure 23. Password Recovery Option in File Menu

2. Contact Pelco Product Support with the following information:
   a. MAC address as it appears in the Password Recovery dialog box.
   b. Current date for your location as it appears in the Password Recovery dialog box.
   c. Any additional information requested by Pelco Product Support

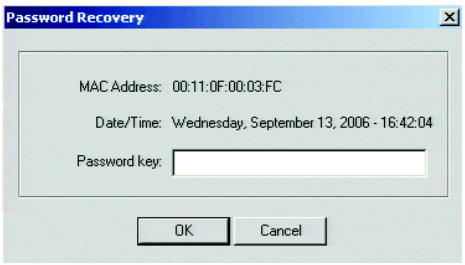

Figure 24. Password Recovery Dialog Box

3. Enter the new password you obtained from Pelco Product Support in the field provided.
4. Click OK.

DX8100 System Recovery Procedure

This DX8100 recovery procedure is used in two ways:

- To recover your DX8100 software using the DX8100 Recovery DVD that is provided with the unit.
- To recover your DX8100 Series DVR in case of a catastrophic failure. In this case, this procedure should only be thought of as a last resort endeavor. The recovery process erases the entire contents of your DVR's primary hard disk drive and overwrites the disk with a fresh image of the system and application software from the DX8100 Recovery procedure.

NOTE: To save the DVR settings before performing the recovery procedure, record the network settings and export and import the DVR settings.

The steps for performing a recovery procedure are summarized as follows:

1. Record the DX8100 network settings.
2. Export the DX8100 settings, to save your camera properties, schedules, and user configurations.
3. Record the IPSec setting.
4. Perform the DX8100 recovery procedure.
5. Perform only the DX8100 import procedure to import the camera properties, schedules, and user configurations that you saved in step 2.

SAVING DVR SETTINGS

RECORDING NETWORK SETTINGS

1. From the DX8100 toolbar, click the Setup icon.
2. Click the Network icon and do the following:
   a. Record the DX8100 IP address: _____.
   b. Record the subnet mask: _____.
   c. Record the default gateway address: _____.
   d. Indicate if "Obtain an IP Address Automatically" is: Checked_____ Unchecked_____.
   e. If Enable Multicasting is selected, record the multicast group IP address_____.

EXPORTING DVR DX8100 SETTINGS

1. Insert a USB key into one of the DX8100 USB ports on the front panel.
2. Click Edit > Export Setup.
3. Double-click the drive assigned to your USB key.
4. Type a name for your backup file in the File name text box, and then click Save. The DX8100 exports the settings to the USB key.

   NOTE: Allow 60 seconds for the export process to finish to ensure that all of the DX8100 settings are exported before performing the recovery procedure.
5. To stop the USB device, do the following:
   a. From the DX8100 menu, click File > Unplug/Eject Hardware. The Unplug or Eject Hardware dialog box opens.
   b. Click Stop. The "Stop a Hardware device" dialog box opens.
   c. Select the USB device to which the DX8100 settings are exported.
   d. Click OK. The "Safe to Remove Hardware" dialog box opens.
   e. Click OK.
   f. Click Close.
6. Unplug the USB key.

RECORDING IP SECURITY SETTINGS

1. Exit the DX8100 application window to the Windows environment.
2. On the taskbar, click Start, and then click Programs > Manage IPSec Policy.
3. Record the status of Enable IP Security Policy: Checked_____ Unchecked_____.
4. Click Cancel to exit.

RUNNING THE DX8100 RECOVERY PROCEDURE

To reinitialize your DX8100 Series DVR and reinstall all operating system and application software:

1. Insert the DX8100 Recovery DVD into the DVD drive.
2. Do the following:
   a. Restart the DX8100.
   b. Enter the BIOS by pressing Delete at the point the Pelco splash screen is displayed. The BIOS Setup UTILITY opens.

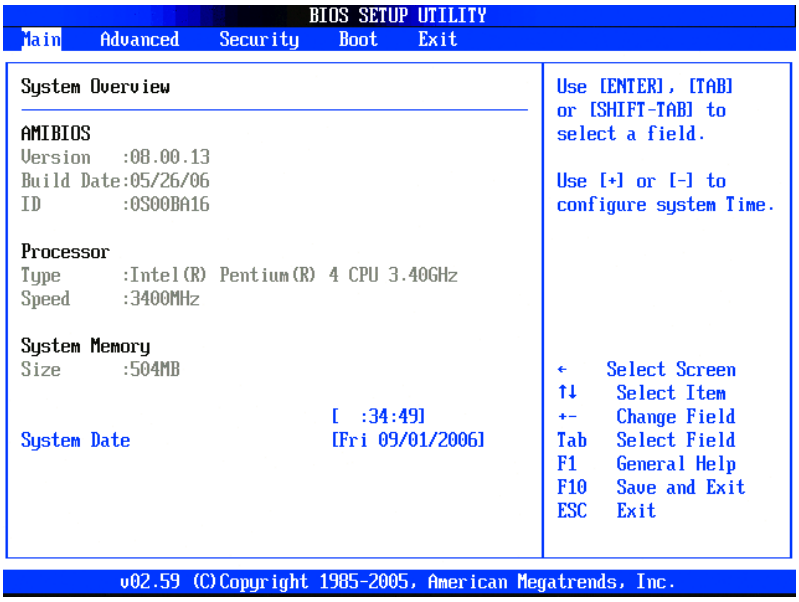

Figure 25. DX8100 BIOS Setup Main Screen

c. In the BIOS setup, go to the Boot tab, select Boot Device Priority, and then press Enter. The Boot Settings page is displayed.

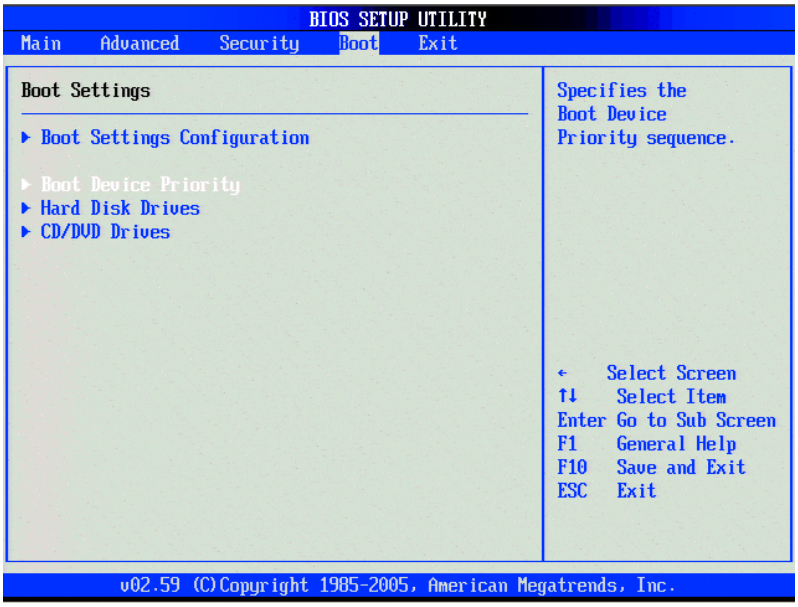

Figure 26. Boot Settings Page

d. In the Boot Settings page, select Boot Devices Priority. and press Enter. The Boot Device Priority page is displayed.

e. In the Boot Device Priority page, press the keyboard + key until CD/DVD is #1 in the list.

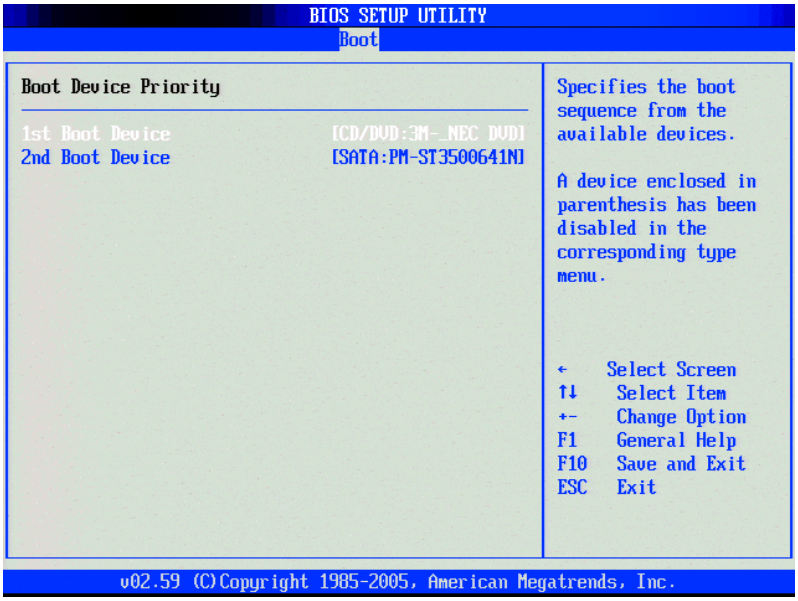

Figure 27. Moving the CD/DVD Device to be First in List

f. Press F10 and then select OK to save your changes and exit. The DX8100 will restart and prompt you by displaying “Press any key to boot from CD.”

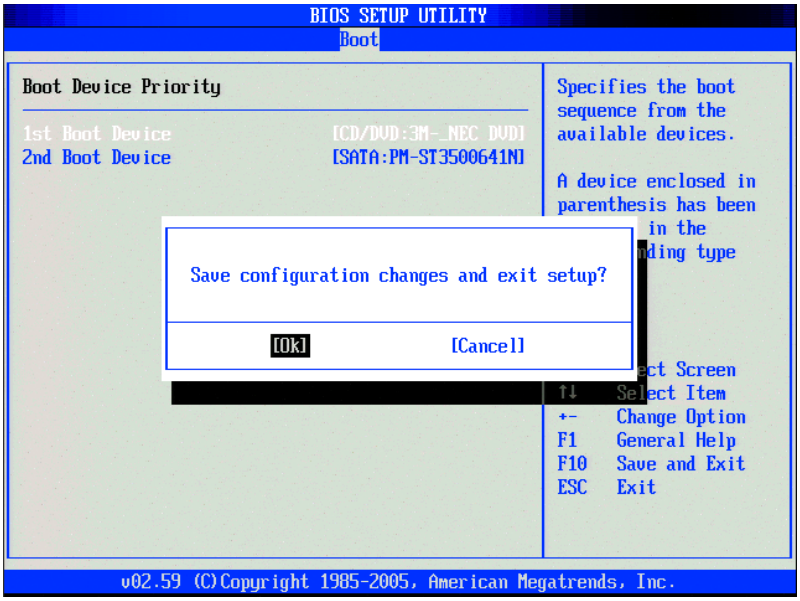

Figure 28. Selecting OK to Save Changes

NOTE: The prompt “Press any key to boot from CD/DVD” appears for only a few seconds, and if missed the unit will not boot from the DX8100 Recovery DVD.

g. Press the Space bar. After the DVD finishes loading, one of the following will occur:

- If using Windows XP Embedded, the End User License Agreement (EULA) appears. Go to step h.
- If using Windows 2000, the DX8100 Recovery dialog box opens. Go to step i.

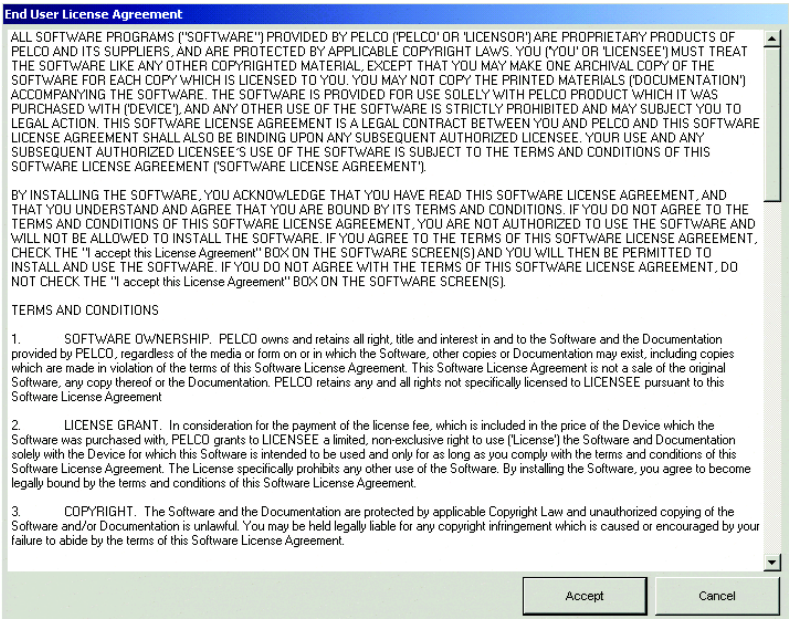

Figure 29. End User License Agreement Dialog Box

h. Do one of the following:

- To accept the EULA, click Accept. The DX8100 Re-Install dialog box opens, displaying the Warning message. Go to step i.
- To Cancel the reinstallation process, click Cancel. The DX8100 restarts.

i. Type **Yes** in the text box to agree to the recovery procedure, and then click Proceed.

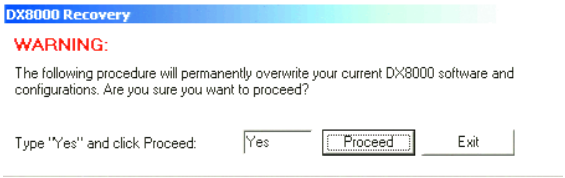

Figure 30. Warning Message and Recovery Configuration

j. Wait while the recovery process starts.

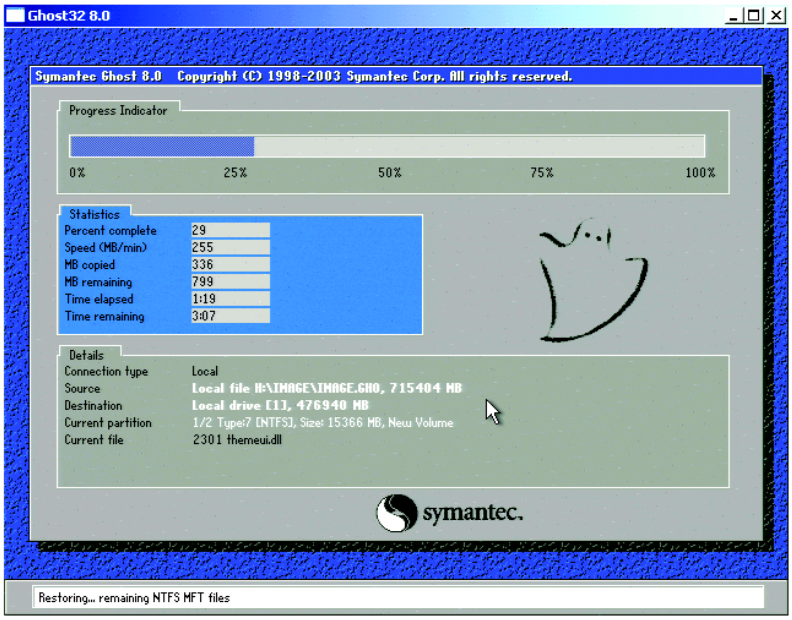

Figure 31. Recovery Process Progress Indicator shows Status

k. After the recovery process has completed, the system displays the DX8100 Re-Install Finished dialog box. Click Exit to restart the DX8100. The unit restarts.

3. Do the following:

   a. Enter the BIOS by pressing Delete at the point the Pelco splash screen is displayed. The BIOS Setup opens.

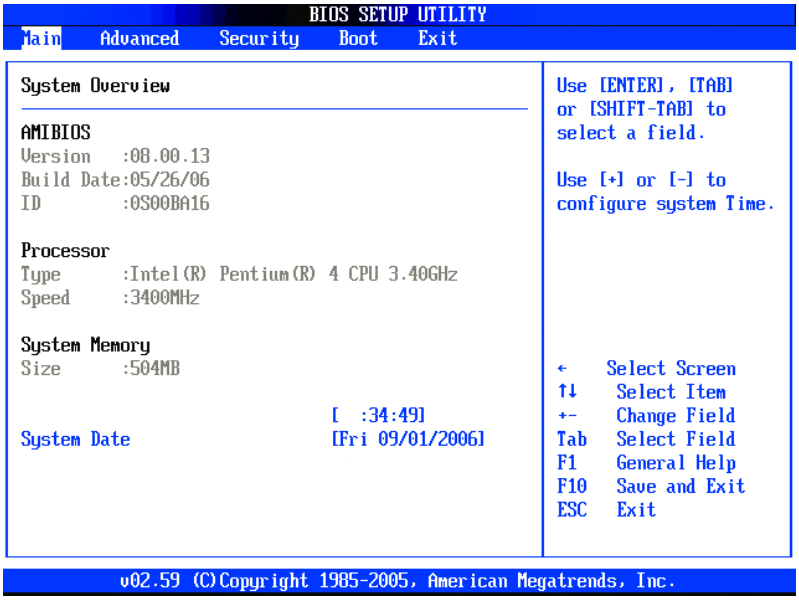

Figure 32. BIOS Setup Window

   b. In the BIOS setup, go to the Boot tab, select Boot Device Priority, and then press Enter. The Boot Settings page is displayed.

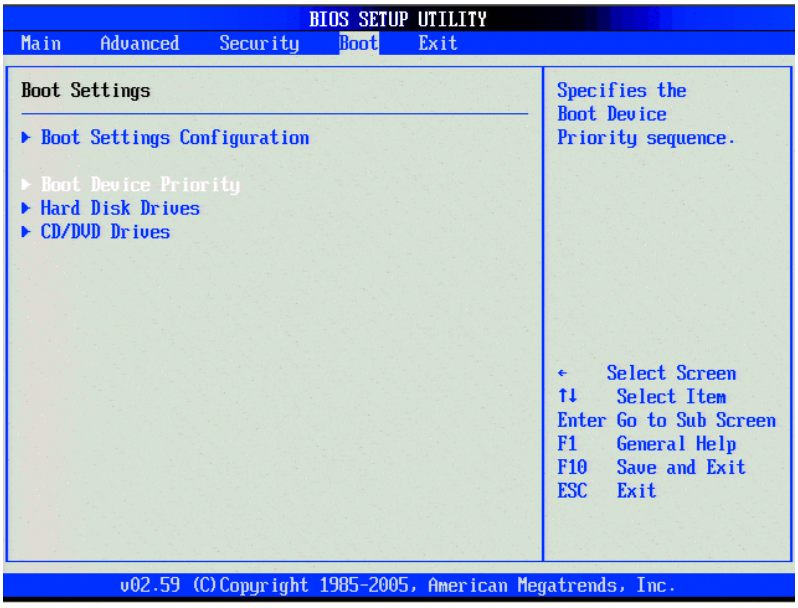

Figure 33. BIOS Boot Settings Page

c. In the Boot Settings page, select Boot Devices Priority. and press Enter. The Boot Device Priority page is displayed.

d. In the Boot Device Priority page, select SATA, and press + until SATA appears first in the list.

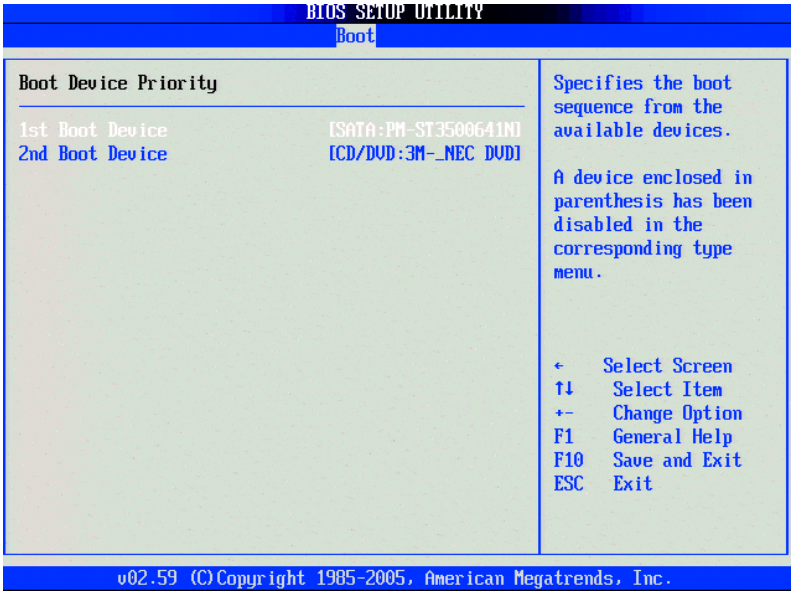

Figure 34. Boot Device Priority Page

4. Eject the DX8100 Recovery DVD.

5. Press F10, and then select OK to save the changes and exit. The DX8100 will reboot and prompt you to initialize the hard disks for use with the DX8100 database.

6. Click the plus sign (+) next to the PDB Group ID box to expand the tree.

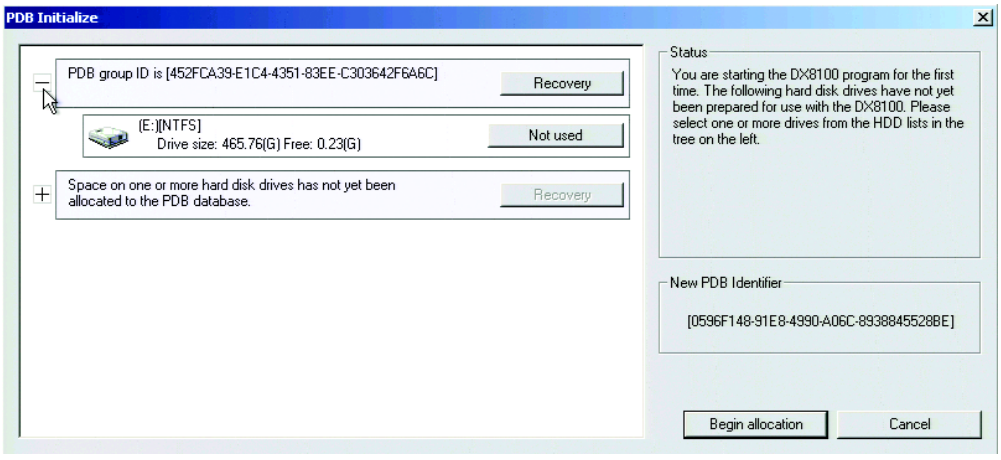

Figure 35. Expanding PDB Tree

- If you are updating an existing system and you want to save previously recorded video, select Recovery on the PDB Group ID box. In this case, all of the boxes should turn yellow and the individual drives should have Used selected. This step will save your recorded video.

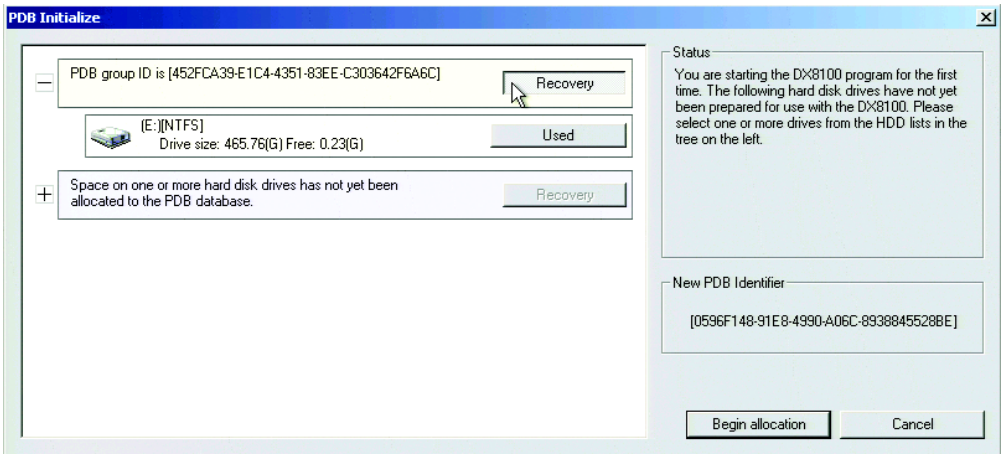

Figure 36. PDB Initialization Screen with Recovery Active

- If you are installing this system for the first time, make sure that Allocation is selected on each of the individual disk drives in the tree. This step will erase all data on all of the drives.

7. Click Begin Allocation to start the database initialization. Depending on the drive configuration, the DX8100 will take between 5 and 15 minutes to initialize the database and begin operation.
8. *Important:* Perform the following steps immediately after the DX8100 completes the initialization process, restarts, and begins operation.
   a. From the DX8100 toolbar, click the Setup icon.
   b. Click the System icon
   c. In the Date/Time Setup area of the System Setup page, verify that the DX8100 date, time, and time zone settings are correct.

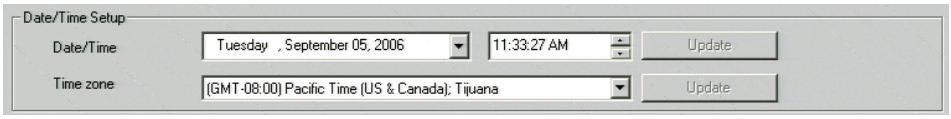

Figure 37. DX8100 System Page Date/Time Setup Area

RESTORING THE DVR SETTINGS

ENTERING NETWORKING SETTINGS

NOTE: If "Obtain an IP Address Automatically" was previously selected, skip this section.

1. From the DX8100 toolbar, click the Setup icon.
2. In the Setup dialog box, click Network.
3. Deselect "Obtain an IP Address Automatically."
4. Type the IP address, subnet mask, and default gateway address that you previously recorded.
5. If applicable, enter the multicast group IP address.

IMPORTING THE DX8100 DVR SETTINGS

1. Insert the USB Key into the front of the unit.
2. Click Edit > Import Setup.
3. Double-click the last drive on the list; this is your USB Key.
4. Locate the backup file you previously created, and then click Open. Your previously backed up settings will now be imported into your new installation.

   NOTE: Allow 60 seconds for the import process to complete before performing step 5. This ensures that all of the DX8100 settings are imported.

5. To stop the USB device, do the following:
   a. From the DX8100 menu, click File > Unplug/Eject Hardware. The Unplug or Eject Hardware dialog box opens.
   b. Click Stop. The Stop a Hardware device dialog box opens.
   c. Select the USB device to which the DX8100 settings are exported.
   d. Click OK. The Safe to Remove Hardware dialog box opens.
   e. Click OK.
   f. Click Close.
6. Unplug the USB key.

CONFIGURING IP SECURITY SETTINGS

NOTE: If Enable IP Security Policy was previously selected, skip this section.

To configure the IP security settings:

1. Do the following:
   a. Click File > Exit. The "Shut down" dialog box opens.
   b. Select Exit to Windows Mode from the drop-down menu. The Log On to Windows dialog box opens.
   c. Enter the Windows operating system user name. (The default user name is DX8100ADM.)
   d. Enter the Windows operating system password. (The default password is dx8100.)
   e. Click OK. The system logs you on to the Windows operating system.
2. When in the Windows operating system environment, do the following:
   a. Click Start on the Windows operating system taskbar.
   b. Click Programs > Manage IPSec Policy. The DX8100 IPSec Policy dialog box opens.
   c. Click the Enable IP Security check box (if it is selected) to deselect it.
   d. Click OK.
3. Do the following:
   a. Click Start.
   b. Click Shut Down. The Shut Down Windows dialog box opens.
   c. Select Restart from the drop-down menu.
   d. Click OK. The DX8100 restarts.

PRODUCT WARRANTY AND RETURN INFORMATION

WARRANTY

Pelco will repair or replace, without charge, any merchandise proved defective in material or workmanship **for a period of one year** after the date of shipment.

Exceptions to this warranty are as noted below:

- Five years on fiber optic products and TW3000 Series unshielded twisted pair transmission products.
- Three years on Spectra® IV products.
- Three years on Genex® Series products (multiplexers, server, and keyboard).
- Three years on Camclosure® and fixed camera models, except the CC3701H-2, CC3701H-2X, CC3751H-2, CC3651H-2X, MC3651H-2, and MC3651H-2X camera models, which have a five-year warranty.
- Three years on PMCL200/300/400 Series LCD monitors.
- Two years on standard motorized or fixed focal length lenses.
- Two years on Legacy®, CM6700/CM6800/CM9700 Series matrix, and DF5/DF8 Series fixed dome products.
- Two years on Spectra III™, Esprit®, ExSite®, and PS20 scanners, including when used in continuous motion applications.
- Two years on Esprit and WW5700 Series window wiper (excluding wiper blades).
- Two years (except lamp and color wheel) on Digital Light Processing (DLP®) displays. The lamp and color wheel will be covered for a period of 90 days. The air filter is not covered under warranty.
- Eighteen months on DX Series digital video recorders, NVR300 Series network video recorders, and Endura™ Series distributed network-based video products.
- One year (except video heads) on video cassette recorders (VCRs). Video heads will be covered for a period of six months.
- Six months on all pan and tilts, scanners or preset lenses used in continuous motion applications (that is, preset scan, tour and auto scan modes).

Pelco will warrant all replacement parts and repairs for 90 days from the date of Pelco shipment. All goods requiring warranty repair shall be sent freight prepaid to Pelco, Clovis, California. Repairs made necessary by reason of misuse, alteration, normal wear, or accident are not covered under this warranty.

Pelco assumes no risk and shall be subject to no liability for damages or loss resulting from the specific use or application made of the Products. Pelco's liability for any claim, whether based on breach of contract, negligence, infringement of any rights of any party or product liability, relating to the Products shall not exceed the price paid by the Dealer to Pelco for such Products. In no event will Pelco be liable for any special, incidental or consequential damages (including loss of use, loss of profit and claims of third parties) however caused, whether by the negligence of Pelco or otherwise.

The above warranty provides the Dealer with specific legal rights. The Dealer may also have additional rights, which are subject to variation from state to state.

If a warranty repair is required, the Dealer must contact Pelco at (800) 289-9100 or (559) 292-1981 to obtain a Repair Authorization number (RA), and provide the following information:

1. Model and serial number
2. Date of shipment, P.O. number, Sales Order number, or Pelco invoice number
3. Details of the defect or problem

If there is a dispute regarding the warranty of a product which does not fall under the warranty conditions stated above, please include a written explanation with the product when returned.

Method of return shipment shall be the same or equal to the method by which the item was received by Pelco.

RETURNS

In order to expedite parts returned to the factory for repair or credit, please call the factory at (800) 289-9100 or (559) 292-1981 to obtain an authorization number (CA number if returned for credit, and RA number if returned for repair).

All merchandise returned for credit may be subject to a 20% restocking and refurbishing charge.

Goods returned for repair or credit should be clearly identified with the assigned CA or RA number and freight should be prepaid. Ship to the appropriate address below.

If you are located within the continental U.S., Alaska, Hawaii or Puerto Rico, send goods to:

Service Department
Pelco
3500 Pelco Way
Clovis, CA 93612-5699

If you are located outside the continental U.S., Alaska, Hawaii or Puerto Rico and are instructed to return goods to the USA, you may do one of the following:

If the goods are to be sent by a COURIER SERVICE, send the goods to:

Pelco
3500 Pelco Way
Clovis, CA 93612-5699 USA

If the goods are to be sent by a FREIGHT FORWARDER, send the goods to:

Pelco c/o Expeditors
473 Eccles Avenue
South San Francisco, CA 94080 USA
Phone: 650-737-1700
Fax: 650-737-0933

Green The materials used in the manufacture of this document and its components are compliant to the requirements of Directive 2002/95/EC.

REVISION HISTORY

Manual #	Date	Comments
C2641M	9/06	Original manual.
C2641M-A	9/07	Added section about changing the Windows XP Embedded administrator password, revised the DX8100 security information, antivirus section, and updated system recovery procedure for Windows XP Embedded.

Worldwide Headquarters
3500 Pelco Way
Clovis, California 93612 USA

USA & Canada
Tel: 800/289-9100
Fax: 800/289-9150

International
Tel: 1-559/292-1981
Fax: 1-559/348-1120

www.pelco.com

ISO**9001**

Australia | Canada | Finland | France | Germany | Italy | Macau | The Netherlands | Russia | Singapore
South Africa | Spain | Sweden | United Arab Emirates | United Kingdom | United States